PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32, H04M 1/66

A1

(11) International Publication Number: WO 98/28877

(43) International Publication Date: 2 July 1998 (02.07.98)

(21) International Application Number: PCT/FI97/00793

(22) International Filing Date: 17 December 1997 (17.12.97)

(30) Priority Data:
965138 20 December 1996 (20.12.96) FI

(71) Applicant *(for all designated States except US)*: NOKIA MOBILE PHONES LTD. [FI/FI]; Keilalahdentie 4, FIN–02150 Espoo (FI).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: HONKANEN, Jukka–Pekka [FI/FI]; Opiskelijankatu 18 A 16, FIN–33720 Tampere (FI). EROLA, Mika [FI/FI]; Ylioppilaankatu 7 C 35, FIN–33720 Tampere (FI). TAMSKI, Markku [FI/FI]; Sammonkatu 27 E 73, FIN–33540 Tampere (FI).

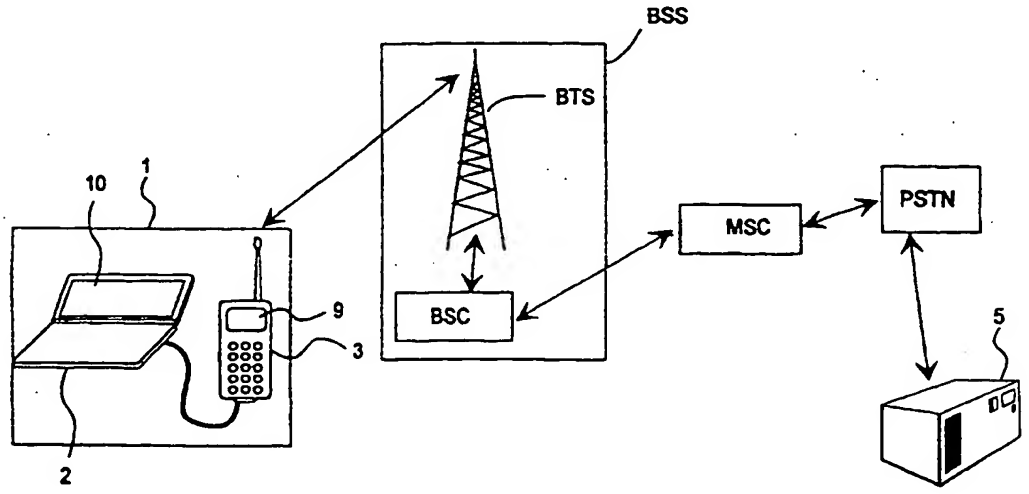
(74) Agents: PURSIAINEN, Timo et al.; Tampereen Patenttitoimisto Oy, Hermiankatu 6, FIN–33720 Tampere (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

BEST AVAILABLE COPY

(54) Title: METHOD FOR IDENTIFICATION OF A DATA TRANSMISSION DEVICE



(57) Abstract

In a method for identification of a data transmission device (1, 5) in a data transmission system, a data transmission connection is formed between at least a first (1) and a second data transmission device (5). The identification is conducted two ways, wherein the second data transmission device (5) identifies the first data transmission device (1) and the first data transmission device (1) identifies the second data transmission device (5). The identification comprises at least the following steps: generating at least one identification message (R1, R2), transmission of said identification message (R1, R2) between the data transmission devices (1, 5), generating a check–up message (C1s, C2p) of said identification message (R1, R2) in the receiving data transmission device (1, 5), sending said check–up message (C1s, C2p) to the data transmission device (1, 5) which sent the identification message (R1, R2), in which a verification message (C1p, C2s) is generated, with which the received check–up message (C1s, C2p) is compared.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Method for identification of a data transmission device

The present invention relates to a method presented in the preamble of Claim 1 for identification of a data transmission device in a data transmission system, where a connection is made for transmission of data between a first data transmission device and a second data transmission device. The invention relates also to a data transmission system presented in the preamble of Claim 5 and to a data transmission device presented in the preamble of Claim 8.

Systems have been developed for making various payments by data processing equipment, by telecommunication terminal equipment, such as a telephone or a mobile station, by a payment terminal, or by a so-called smart card (processor card). Particularly the payment transactions of companies are nowadays largely made through data processing equipment of the company itself, wherein the data processing equipment has banking software or the like for input of the payments. Thus a terminal is used for input of the required information, such as the bank account number of the recipient, the sum in marks, the due date etc., wherein the data processing equipment makes a data transmission connection, for example via a modem and a telecommunication network, to the data processing equipment handling payments at a bank, such as mainframe. For preventing misuse, the payer must enter his or her user identification code and password at the beginning of the connection, wherein the data processing equipment of the bank checks if the given data correspond with the data recorded in the data processing equipment of the bank. If the data are identical, the data processing equipment of the bank will start receiving data and record the payments in its register and transfer the given sum of money on the due date from the account of the payer to the account of the recipient.

For payment, the data transmission is usually made either by batch processing or in real time. In batch processing, the data of all the payments to be made at a time are set in the memory of the data processing device, whereafter a data transmission connection is made with the payment server of the bank and the data is transmitted. After the transmission, the connection can be cut. Thus connection time is es-

sentially used only as long as is required for data transmission at the transmission rate available at the time. In real-time transmission, the connection is made as early as at the beginning of the session and the payment data are transmitted immediately to the payment server of the bank. After the payment instructions are entered and sent to the payment server of the bank, the connection is cut. This alternative requires a longer connection time than batch processing.

So-called smart cards or processor cards are small cards manufactured usually in the size of a credit card and having a microprocessor and electronic circuits required for its operation laminated in plastic. Further, the surface of the card is usually provided with electric contacts for connecting supply voltages to the card and for transferring control and data signals between the card and its read/write device. However, systems have been developed for transferring the signals between the card and its read/write device as well as the supply voltages of the card in a wireless manner e.g. as high frequency electromagnetic signals. These methods involve the problem of transmitting a sufficiently high quantity of energy to the card so that the card can perform the necessary operations, such as checking of encryption and decryption, sufficiently quickly.

Smart cards are used e.g. as charge cards in several different applications, such as with public telephones, as coin cards, as means of payment at public transportation means, etc. When a smart card is to be used as a charge card, money can be stored on its so-called electronic purse for example at automatic cash dispenser points having the equipment for controlling the smart card and charging money on the card.

Figure 1b is a reduced block diagram illustrating the internal structure of a smart card 12, known as such. A central processing unit CPU controls the operation of the smart card 12 on the basis of a program code stored in the read-only memory ROM. Various user-specified data to be stored permanently in the memory can be stored in the electrically erasable programmable read-only memory EEPROM. During use of the smart card, the data memory RAM can be used as a temporary data storage. A bus adapter DATA-I/O adapts the smart card 12 to the inter-

face lines of the card reading device (not shown) as well as to a control and data line 13. The properties and function of the smart cards can be set by storing application software according to the use in the program memory of the card advantageously at the manufacturing stage.

Increased popularity of the Internet data network has given particular rise to the development of various payment systems in which the user of the Internet network can for example order goods from different suppliers and make payments for the orders by using the Internet data network. In addition to making orders and payments, the Internet data network and other data transmission systems are used to carry messages and even confidential information. Thus the sender and receiver of the message should be able to make sure that the other party of the connection is really the intended one. However, it is very easy to eavesdrop the Internet data network and to follow communication in it, wherein it is also possible to forge and misuse data. It should still be possible to make payments and transmit other confidential information in a way that is protected as well as possible from outsiders. For enciphering communication, enciphering or encryption systems have been developed for data transmission systems as well as identification systems for identification of the sender of the information e.g. in connection with making payments. The encryption methods are primarily based on the fact that each user has his or her own user code and an encryption key for confirming the identification of the user. This confirmation with the encryption key is also called digital signature, because this method is analogous to the situation in which the user pays for purchases e.g. with a credit card and confirms his or her identity with his or her own signature which the seller possibly compares with the signature on the I.D. card or the like of the payer.

The purpose of the digital signature is thus to identify both the user and the transmitted message and to secure that the content of the message has not changed during the transmission. Using the digital signature enhances security of smart card systems and other systems and other systems based on electronic payment.

There are two main types of digital signature systems: those based on a secret key and those based on a public key.

In a system based on the secret key, the same encryption key is used for forming the digital signature at the sending end and for confirming the transmitted signature at the receiving end, wherein the operations for both encryption and confirming are substantially identical. The secret key system is also called symmetric encryption. One very well known encryption method using a secret key is the U.S. Federal Data Encryption Standard (DES). The encryption can involve either all the transmitted data or only some of the data, such as the user code. The encrypted information is known to the communication parties, or the encryption data is marked in the data to be transmitted e.g. by changing the value of an encryption bit. Thus it is possible at the receiving end to find out which parts of the received data are encrypted. At the receiving stage, an encryption checking key identical to the encryption key is used for confirming that the received encrypted information is correct, i.e. the encryption key used at the transmitting stage was identical with the encryption checking key used at the receiving stage. The encryption can be deciphered by using the encryption checking key.

In encryption systems based on a public key, a pair of two keys is used, the first being a secret key and the second a public key. The secret key is used for encrypting the data to be encrypted at the transmission stage, and the encryption is checked using the public key at the receiving stage. The public key can be used only for checking the encryption and for deciphering, but it is not possible to use the public key to find out which encryption key was used to encrypt the data. The system based on a public key is also called asymmetric encryption. In this system, the public key can be known to anybody, but the secret key is only known to the sender.

Consequently, systems based on the secret key require that the same encryption key is known both to the sender and the receiver. Thus for example in payment terminal applications, the payment terminal must contain the encryption keys of all the persons having the right to use the payment terminal, wherein such a payment terminal must be made very reliable and crack-proof. In practice, this means that the apparatus becomes very expensive and it must be mounted on its ground in a stationary manner and possibly also equipped with a burglar alarm or

the like. In this respect, the public key system is more advantageous, because the payment terminal or the like does not need to contain secret keys but it is sufficient that the terminal has the public keys for checking the encryption made with different encryption keys. For each public key there can be several secret keys, wherein the number of keys to be stored is substantially smaller than in systems based on the secret key. Further, it is not possible to use the public key to find out the encryption key used for encryption. On the other hand, the above-mentioned encryption methods have the disadvantage that the sender cannot make sure that the receiver is the intended recipient. There is thus the risk of an outsider to interfere with the data transmission e.g. by coupling on telephone lines and forging data transmission. Furthermore, this can be performed in a way that both the sender and the intended recipient see the situation as normal but in reality the communication is made via a third party and the payment can be directed to a wrong account or confidential information is made known to outsiders.

In mobile communication networks at least part of the data transmission is made in a wireless manner by using radio transmitters and receivers. The radio channel is a physically open resource which is available to anybody via suitable data transmission device. This involves security risks, for example eavesdropping or disclosure of the privacy of a location. In digital mobile communication networks, such as GSM networks, digital data transmission is used which is difficult to eavesdrop. Further, it is possible to use caller identification and encryption in data transmission. For preventing eavesdropping, encryption methods have been developed for digital mobile communication networks, whereby the speech converted to digital form and the data signal are encrypted. Also other information carried via the radio channel can be encrypted, such as the identification data of a mobile station (International Mobile Subscriber Identity, IMSI) and the identification data on the location (Location Area Identification, LAI). In the receiver, the encrypted signal is deciphered back to unencrypted speech and data. The encryption key and algorithm to be used in encryption is advantageously known only to the sending and receiving equipment in question, wherein the deciphering of the coded signal to intelligible speech and data as well as to processing signals of the bit stream in a violent or illegal manner

without the correct encryption key and algorithm is very difficult, thanks to the efficient encryption algorithms currently in use.

At present, mobile stations are known which use a smart card of the type shown in Figure 1a, comprising a subscriber identity module, such as a SIM module 4. The SIM module comprises typically a central processing unit (CPU), a read-only memory (ROM), an electrically erasable programmable read-only memory (EEPROM), and a random access memory (RAM). For using the mobile station, a personal identity code stored on the SIM module must be given in connection with the use of the mobile station, usually upon switching on the mobile station. The data memory of the SIM module can also be used for storing other user-specified information, telephone numbers, messages, etc.

The most common digital mobile communication networks are so-called cellular networks. Figure 2 is a reduced diagram showing a mobile communication network known as such, in which the invention can be advantageously applied. The base station subsystem (BSS) of the mobile communication network comprises base transceiver stations (BTS) and base station controllers (BSC). The mobile station (MS) 3 is in a data transmission connection via the radio channel with a base station close to the respective location of the mobile station. The base station is in a data transmission connection with the base station controller. Data transmission between the base station and the base station controller is usually carried via a cable. Each base station controller operates with a group of several base stations. The base station controller is, in turn, in a data transmission connection with a mobile services switching center (MSC). The mobile services switching centers can, in turn, be in a data transmission connection with each other as well as with a landline communication network center (PSTN, ISDN). The information to be transmitted is usually divided into frames containing control information, speech converted to digital form, data, and error correction information. The frame structure can have several levels, wherein the frames of an upper level are formed by arranging frames of a lower level. Encryption can be directed both to the control information and the speech and data portions. Further, the encryption can be carried out also in a way that different encryption keys and algorithms are used at different frame levels. One example of digital communica-

tion networks is the GSM network which has a standard defining the encryption methods and algorithms to be used.

In the GSM network, a mobile originated call is set up in a way that the GSM mobile station and the GSM system network send control and identification signals required for call set-up to each other. In response to a connection request, the GSM mobile station is assigned a channel for signalling, if this is possible within the capacity of the GSM system network. On this channel, the GSM mobile station makes the GSM system network a request for speech or data services. On the side of the GSM system network, this request is transmitted to the mobile services switching centre (MSC), in which the rights of the GSM subscriber in question are verified from the visitor location register (VLR).

Upon a mobile terminated call e.g. from a landline telephone network subscription, the PABX of the telephone network transmits *inter alia* the telephone number of the mobile station to the mobile services switching centre. The MSC verifies the rights of the GSM subscriber in question from the home location register (HLR) and the visitor location register (VLR). Following this, the GSM system network and the GSM mobile station send control and identification data required for call set-up.

Depending on the application and on the configuration of parameters, the visitor location register VLR can, via the mobile services switching centre, send the GSM mobile station a request for exchange of identification data and start of encryption. However, call set-up is possible also without exchange of identification data and encryption. In other words, the call is either encrypted or not encrypted according to the network parameters set by the operator of the GSM system network.

In the GSM system, encryption is made on the physical level as bit-specified encryption, i.e. the bit stream to be transmitted on the radio channel is formed by adding to the data the encryption bits that are generated by the A5 algorithm, known as such, using the encryption key Kc. The A5 algorithm encrypts on the physical level the data and signalling information to be transmitted on channels assigned for data transmission (traffic channel, TCH, or dedicated control channel, DCCH).

Synchronization of the messages to be transmitted is secured by controlling the A5 algorithm with specific synchronization data (COUNT). The synchronization data COUNT is formed on the basis of the TDMA frame number. Thus the content of each 114 bit block generated with the A5 algorithm depends only on the frame numbering and the encryption key Kc.

The encryption key Kc is preferably set up at the stage when the communication on the assigned channel is not yet encrypted and the mobile communication network to be used has identified the mobile station MS. In the GSM system, the mobile station is identified by using the international mobile subscriber identity (IMSI) stored in the mobile station, or by using a temporary mobile subscriber identity (TMSI) formed on the basis of the subscriber identity. There is also a subscriber identification key Ki stored in the mobile station. This subscriber identification key Ki is also known to the mobile communication network.

For ensuring that the encryption key Kc is known to the mobile station MS and the mobile communication network only, the encryption key is transmitted indirectly from the base station subsystem BSS to the mobile station MS. Thus a random access number RAND is given by the base station subsystem BSS and sent to the mobile station MS. The encryption key Kc is generated by the algorithm A8 from the random access number RAND and the subscriber identification key Ki of the mobile station. The calculation and storing of the encryption key Kc is performed both in the mobile station MS and in the mobile communication network.

At the beginning of the connection, communication between the mobile station MS and the base station subsystem BSS is unencrypted. The transfer to the encryption mode is advantageously made in a way that the base station subsystem BSS sends the mobile station a certain command (unencrypted) which in this context is called "start cipher". After the mobile station MS has received the "start cipher" command, it starts encryption of the messages to be transmitted and deciphering of received messages. In a corresponding manner, the base station subsystem BSS starts encryption of messages to be sent to the mobile sta-

tion after the base station subsystem has received an encrypted message sent by the mobile station and deciphered it correctly.

Consequently, the identification and encryption information is transmitted one-way, from the base station subsystem to the mobile station, wherein the base station subsystem does not confirm that the mobile station MS is the correct mobile station. Also, the mobile station MS does not necessarily know that the messages sent from the mobile station MS are transmitted to the correct base station subsystem. Thus there exists the possibility that efficient calculating devices and data transmission device can be used to intercept messages from the communication between the base station subsystem BSS and the mobile station MS.

It is an aim of the present invention to eliminate all the above-mentioned disadvantages to a major extent and to provide a data transmission system where the communicating parties can identify each other in a reliable way to prevent possible misuse. The invention is based on the idea that the identification is carried out in the communication both ways advantageously so that both communicating parties identify each other. The method of the present invention is characterized in what will be presented in the characterizing part of the appended Claim 1. The system of the present invention is characterized in what will be presented in the characterizing part of the appended Claim 5. Further, the device of the present invention is further characterized in what will be presented in the characterizing part of the appended Claim 8.

The present invention gives significant advantages to the encryption methods and systems of prior art. According to the invention, double-checking is performed, wherein both parties to the communication session can make sure that the other party is exactly the intended one. Thus it is not possible for outsiders to find out the content of the data to be transmitted and to direct the information to a wrong address. Payment operations are made safer than by using methods and systems known at present.

Checking can be done also during the data transmission connection, wherein attempts during the data transmission connection to interfere

with the data to be transmitted can be found out and data can be prevented from falling into the hands of outsiders.

The invention will be described in more detail in the following with reference to the appended drawings. In the drawings,

Fig. 1a shows a smart card,

Fig. 1b is a reduced block diagram showing the functional structure of a smart card,

Fig. 2 is a reduced diagram showing a mobile communication network known as such,

Fig. 3 shows a communication system according to an advantageous embodiment of the invention,

Fig. 4 is an arrow diagram showing a payment operation according to the invention, and

Fig. 5 is a status chart showing identification according to the invention.

The following example illustrates the use of the method according to the invention for making a order and payment of an article or service in the communication system shown in Fig. 3, such as the Internet data network. The invention can also be applied in other types of data systems and for transmitting other types of data.

The user makes the necessary operations with a first data transmission device 1, which in this advantageous embodiment of the invention comprises at least a first data processor 2, such as a portable computer (PC), a first telecommunication terminal 3, which is e.g. a mobile station MS, such as a GSM mobile station, and a SIM module 4. The first data processor 2 is in data transmission connection with the first telecommunication terminal 3. The SIM module 4 is also in a data transmission connection either with the first data processor 2, the first telecommunication terminal 3, or both. The SIM module 4 can also be

part of the first telecommunication terminal 3, such as is known from GSM mobile stations. The first data processor 2 and the first telecommunication terminal 3 shown in Fig. 3 can be either separate devices or they can be integrated as for example in the Communicator manufactured by Nokia.

The invention will be described using the SIM module 4 as an electronic purse, as shown in Fig. 3, but the electronic purse can also be a charge card or the like. Thus, for applying the invention, the operations required in the SIM module can be provided at least partly also in the charge card or the like.

A second data transmission device 5 comprises advantageously a second data processor 6 which is e.g. a mainframe of the bank (payment server), a second telecommunication terminal 7, such as a modem, and a security access module (SAM) 8 for checking the user rights. The second data processor 6 and the second telecommunication terminal 7 are in data transmission connection with each other for transmitting messages between the second data processor 6 and a communication network 11. The SAM module 8 is coupled advantageously to the second data processor 6.

In the first data transmission device 1, the SIM module 4 makes the operations required for identification of the data transmission parties and also for encryption of data transmission in the data transmission device 1, as well as deciphers the encrypted data received from the second data transmission device 5. In a corresponding manner in the second data transmission device 5, the SAM module 8 makes the operations required for identification of the data transmission parties and also for encryption of data transmission in the second data transmission device 5, as well as deciphers the encrypted data received from the first data transmission device 1.

Encryption of the data to be transmitted is made advantageously by selecting an encryption algorithm A1, A2, A3, as shown in the status chart of Fig. 5. In the first data transmission device 1, the encryption algorithms A1, A2, A3 are stored preferably in the SIM module 4, and in the second data transmission device 5 advantageously in the SAM

module 8. Thus the encryption algorithm A1, A2, A3 corresponding to the respective stage of identification according to the invention is searched in the application software of the SIM module 4 and the SAM module 8. This is shown by the indices A1, A2, A3 in the respective blocks in Fig. 5. The encryption key K, Kc and the data to be transmitted are used as inputs of the selected encryption algorithm A1, A2, A3, wherein the encryption algorithm A1, A2, A3 generates an encrypted character string (a message), which is known as such. In practical applications of the encryption algorithm, e.g. programmable logic circuits comprising a programmed encryption algorithm can be used, or the encryption algorithm and encryption can be implemented in the application software of the encryption device. In a corresponding manner, also checking of the encrypted data and deciphering can be implemented on the hardware and/or software level. For verification of the encrypted data and deciphering, the same encryption key A1, A2, A3 is used as for encryption. The encryption key K, Kc is either the same as the one used for encryption, or a public encryption key. Thus the input of the algorithm comprises the encrypted data e.g. as a binary character string and the encryption key K, Kc. The result will be information on whether the checked data was encrypted with the correct encryption key K, Kc and encryption algorithm A1, A2, A3.

A payment operation is exemplified in an arrow chart shown in Fig. 4. The operations critical for safety are marked with points in the arrows. For making an order, the user starts e.g. an Internet content browser with the first data processor 2 and finds the www page or the like of the supplier of the goods or services intended. When the correct page has been found and a data transmission connection has been made to the content server of the supplier of the goods or services, the name and order are entered by the user with the first data processor 2 and transmitted to the content server (arrow 401). The content server checks the order and finds the price of the order from its service provider or the like (arrow 402), after which the price information is transmitted to the first data processor 2 (arrows 403, 404), in which advantageously a paymaker shows the price information to the user and requests for a confirmation of order. After the confirmation of order (arrow 405) has been received, the price and the information of the supplier of the goods or services are transmitted from the content

server to a payment server of a bank (arrow 406). After this, the payment operation is started advantageously by setting up a data transmission connection between the first data transmission device 1 and the second data transmission device 5 e.g. as a telephone connection in a situation in which the data transmission connection does not yet exist. In this embodiment, the second data transmission device 5 is the payment server of the bank. Also other known data transmission methods can be used, while the basic idea of the invention remains the same.

We shall next describe identification of data transmission devices according to an advantageous embodiment of the invention. This is illustrated as a status chart in Fig. 5. In the same context, reference is also made to the arrow chart of Fig. 4. In the reference indices C1s, C1p, C2s, C2p of the check-up and verification messages, the last character indicates to the message source in a way that the reference indices of the messages formed in the first data transmission device 1 contain the letter **s** and the reference indices of the messages formed in the second data transmission device 5 contain the letter **p**. The check-up messages C1s, C2p are transmitted between the data transmission devices, but the verification messages C1p, C2s are used within the respective data transmission devices to verify the correctness of the check-up messages.

After the data transmission connection is formed between the data transmission devices 1 and 5, the second data transmission device 5 produces a first identification message R1 advantageously in the SAM module 8 and sends it to the first data transmission device 1 (arrow 407), in which advantageously a paymaker conveys the identification message to the SIM module 4 for processing (arrow 408). The first identification message R1 is advantageously a random character string, wherein it is different at each transmission session, which will further improve reliability of identification and security of data transmission. The first identification message R1 is sent advantageously in unencrypted form. In the first data transmission device 1, the SIM module 4 converts the first identification message R1 to a first check-up message C1s by using a first encryption algorithm A1 and a first encryption key K. Further, the SIM module 4 produces a second identifi-

cation message R2 and converts it to a temporary encryption key Kc by using a second encryption algorithm A2 and a first encryption key K. After this, the first check-up message C1s produced by the SIM module, the second identification message R2 and the identification ID of the SIM module are transmitted to the second data transmission device 5 (arrows 409, 410). The SIM module identification ID is transmitted in unencrypted form, wherein the second data transmission device 5 can select the correct encryption key K on the basis of the SIM module identification ID. The SIM module identification ID can be transmitted in unencrypted form, because outsiders cannot utilize the code without the correct encryption key K.

Now, the SAM module 8 of the second data transmission device 5 knows both the encryption key K and the first encryption algorithm A1. Thus the SAM module 8 makes the corresponding operation to the first identification message R1 as the SIM module 4, i.e. converts the first identification message R1 into the first check-up message C1p by using the encryption key K and the first encryption algorithm A1. Because the operations are identical, also the result, that is the first verification message C1p and the first check-up message C1s, should be identical, if the starting data was the same. The SAM module 8 compares the first check-up message C1s sent from the first data transmission device 1 with the first verification message C1p formed by it. If the comparison shows that these are identical, the SAM module 8 knows that the sender was the first data transmission device 1, or that the data transmission connection is all right in this respect.

Next, the SAM module 8 converts the second identification message R2 sent by the first data transmission device 1 into a second check-up message C2p by using the first encryption algorithm A1 and the encryption key K. Further, the SAM module 8 converts the second identification message R2 into a temporary encryption key Kc by using the second encryption algorithm A2 and the first encryption key K. The price information on the article or service ordered, and the address information of the supplier of said article or service are transmitted to the first data transmission device 1 advantageously in encrypted form. For encryption, the SAM module 8 uses a third encryption algorithm A3 and a temporary encryption key Kc formed by it. The second data

transmission device 5 sends then the price information and the address information in encrypted form as well as the second check-up message C2p to the first data transmission device 1 (arrows 411, 412).

The first data transmission device 1 uses the second identification message R2 produced by the SIM module 4 for producing the second verification message C2s by using the first encryption algorithm A1 and the encryption key K. Consequently, the SIM module 4 makes the corresponding operation to the second identification message R2 as the SAM module 8, wherein the result, i.e. the second check-up message C2p and the second verification message C2s, should be identical, if the starting data was the same. After receiving the second check-up message C2p sent by the second data transmission device 5, the SIM module 4 compares it with the second verification message C2s produced by it. If the result of the comparison is identical to the SIM module 4, the SIM module 4 knows that the transmitter was the second data transmission device 5. After this the SIM module deciphers the received price and address information by using the third encryption algorithm A3 and the temporary encryption key Kc. Now that both parties of the data transmission are identified, the order can be paid.

In connection with the payment operation, the SIM module checks that the sum of money contained in the SIM module 4 is sufficient for making the payment. If there is not sufficiently money loaded in the SIM module 4, the payer can be given an error message for example on the display 9 of the first data transmission device or on the display 10 of the first data processor. If there is sufficiently money stored in the SIM module 4, the sum to be paid is reduced from the money account of the card. The SIM module 4 sends the payment and the identification parameters, encrypted with the third encryption algorithm A3 and the temporary encryption key Kc, to the second data transmission device 5 (arrows 413, 414). The identification parameters used can be for example the payer identification and password for securing that the sent message and the message received by the second data transmission device 5 come from the correct SIM module and that the money is legal.

In connection with the payment, the payment server of the bank transmits an acknowledgement for the payment to the first data transmission device 1 (arrow 415), in which the acknowledgement is transmitted to the SIM module 4 (arrow 416).

The bank payment server sends information on the payment also to the content server (arrow 417). Next, the content server sends the information on the order (e.g. the order number) to the user to the content browser for display of the information (arrow 418). The acknowledgement of receipt of the information by the user is transmitted to the content server (arrow 419) and to the payment server (arrow 420). The content server sends still an acknowledgement of the transmission of the order and payment data via the paymaker (arrow 421) to the SIM module (arrow 422).

Next, the payment server makes the payment in encrypted form to the bank account of the supplier of the article or services, as shown by arrow 423. An acknowledgement of the giro transfer is further sent to the payment server (arrow 424). The order is now received and the payment made.

In the encryption method according to the invention, the encryption key K is required which is linked to the SIM module identification ID. The second data transmission device 5 comprises a data file in which the identifications ID of the SIM modules connected with the system and the corresponding encryption keys K are stored, wherein the second data transmission device 5 is capable of finding out each encryption key K used on the basis of the received SIM module identification ID. Further the method according the invention uses advantageously three encryption algorithms A1, A2, A3. The system implementing the method of the invention is very safe, because the encryption key K and the encryption algorithms A1, A2, A3 are never transmitted via the data network but they are stored in the second data transmission device 5 as well as in the SIM module 4 for example in connection with manufacturing of the SIM module card.

The encryption keys K, Kc, the encryption algorithms A1, A2, A3, the identification messages R1, R2, the check-up messages C1s, C2p, as

well as the verification messages C1p, C2s, and their form, each depend on the application to be used. Typically, digital data transmission systems utilize binary digit strings, whose length is selected according to the use and the properties of the system, e.g. to be divisible by 8 or 16, which is known to an expert in the art.

Although the invention was described above to secure payment operations, the invention can also be advantageously applied for securing communication, wherein the method works substantially in the manner described above. Thus, instead of or in addition to price and address information, data is transmitted which is encrypted with the said encryption key Kc and encryption algorithm A3. Identification of the parties to the data transmission is conducted two ways with the encryption key K, the first encryption algorithm A1 and the two identification messages R1 and R2. The data are transmitted advantageously in packets, wherein in connection with the reception of each packet it can be verified that the packet was sent from the correct sender.

The invention is not limited solely to the above-mentioned embodiments but it can be modified within the scope of the appended claims.

Claims:

1. Method for identification of a data transmission device (1, 5) in a data transmission system, wherein a data transmission connection is formed between at least a first (1) and a second data transmission device (5) and the identification is conducted two ways, wherein the second data transmission device (5) identifies the first data transmission device (1) and the first data transmission device (1) identifies the second data transmission device (5), in which method the identification comprises at least the following steps:

- generating at least one identification message (R1, R2),
- transmission of said identification message (R1, R2) between the data transmission devices (1, 5),
- generating a check-up message (C1s, C2p) of said identification message (R1, R2) in the receiving data transmission device (1, 5),
- sending said check-up message (C1s, C2p) to the data transmission device (1, 5) which sent the identification message (R1, R2), in which
- a verification message (C1p, C2s) is generated, with which the received check-up message (C1s, C2p) is compared,

characterized in that the identifications (ID) of the first data transmission devices (1) that can be linked to the data transmission system as well as the corresponding encryption keys (K) are stored in the second data transmission device (5), wherein the encryption key (K) to be used in generating the check-up message (C1s, C2p) and the verification message (C1p, C2s) is selected on the basis of the identification (ID) of the first data transmission device (1) that is used in the data transmission connection at the time.

2. Method according to Claim 1, **characterized** in that the identification comprises at least the following steps:

- generating the first identification message (R1) at the second data transmission device (5),
- transmission of said identification message (R1) from the second data transmission device (5) to the first data transmission device (1),
- generating the first check-up message (C1s) in the first data transmission device (1),

- transmission of said check-up message (C1s) to the second data transmission device (5), in which
- the encryption key (K) is selected on the basis of the received identification (ID) of the first data transmission device (1),
- the first verification message (C1p) is generated, with which the received check-up message (C1s) is compared,
- the second identification message (R2) is generated at the first data transmission device (1),
- said identification message (R2) is sent from the first data transmission device (1) to the second data transmission device (5),
- the second check-up message (C2p) is generated at the second data transmission device (5), and
- said check-up message (C2p) is sent to the first data transmission device (1), in which
- the second verification message (C2s) is generated, with which the received check-up message (C2p) is compared.

3. Method according to Claim 1 or 2, **characterized** in that an encryption algorithm (A1) and an encryption key (K) are selected, wherein the first check-up message (C1s) is generated from the first identification message (R1) by using the encryption algorithm (A1) and the encryption key (K), and that the second check-up message (C2p) is generated from the second identification message (R2) by using the encryption algorithm (A1) and the encryption key (K).

4. Method according to Claim 1, 2 or 3, **characterized** in that the second identification message (R2), the first check-up message (C1s) and the second verification message (C2s) are generated in a smart card, such as a SIM module (4), arranged in the first data transmission device (1).

5. Data transmission system comprising means (3, 7, 12) for generating a data transmission connection between at least a first (1) and a second data transmission device (5), in which system the data transmission devices (1, 5) are arranged to be identified two ways, wherein the first data transmission device (1) comprises means for identifying the second data transmission device (5) and the second

data transmission device (5) comprises means for identifying the first data transmission device (1), and which identification means comprise:

- means (4, 8) for generating at least one identification message (R1, R2),
- means (3, 7) for transmitting said identification message (R1, R2) between the data transmission devices (1, 5),
- means (3, 7) for generating a check-up message (C1s, C2p) in the data transmission device (1, 5) receiving said identification message (R1, R2), and
- means (4, 8) for sending said check-up message (C1s, C2p) to the data transmission device (1, 5) that sent the identification message (R1, R2), comprising means (4, 8) for generating a verification message (C1p, C2s) and means (4, 8) for comparing the verification message (C1p, C2s) and the received check-up message (C1s, C2p),

characterized in that the second data transmission device (5) comprises further means for storing the identifications (ID) of the first data transmission devices (1) and the corresponding encryption keys (K), wherein the encryption key (K) is arranged to be selected on the basis of the identification (ID) of the first data transmission device (1) being used at the time.

6. System according to Claim 5, **characterized** in that the means for identification of the first data transmission device (1) comprise:

- means (8) for generating the first identification message (R1), the second check-up message (C2p) and the first verification message (C1p),
- means (7) for sending said first identification message (R1) and the second check-up message (C2p) to the first data transmission device (1),
- means (7) for receiving the first check-up message (C1s) of the second identification message (R2) and the identification (ID) of the first data transmission device (1),
- means (8) for selecting the encryption key (K) on the basis of the identification (ID) of the first data transmission device (1), and
- means (8) for comparing the first check-up message (C1s) and the first verification message (C1p),

and that the means for identification of the second data transmission device (5) comprise:

- means (4) for generating the second identification message (R2), the first check-up message (C1s) and the second verification message (C2s),
- means (3) for sending said second identification message (R2) and the first check-up message (C1s) to the second data transmission device (5),
- means (3) for receiving the first identification message (R1) and the second check-up message (C2p), and
- means (4) for comparing the second check-up message (C2p) and the second verification message (C2s).

7. System according to claim 5 or 6, **characterized** in that the means (4) for generating the second identification message (R2), the first check-up message (C1s) and the second verification message (C2s) comprise a smart card, such as a SIM module (4).

8. Data transmission device (1, 5), such as a mobile station, comprising:

- means (4) for storing the identification (ID) of the data transmission device (1),
- means (4) for generating an identification message (R1, R2),
- means (3) for transmitting said identification message (R1, R2),
- means (3) for receiving a check-up message (C1s, C2p) generated on the basis of the transmitted identification message (R1), and
- means (4) for generating a verification message (C1p, C2s) on the basis of the received check-up message (C1s, C2p),

characterized in that it comprises further means (3) for transmitting the identification (ID) of the data transmission device (1) to a second data transmission device (5), wherein in the second data transmission device (5) the encryption key (K) is arranged to be selected on the basis of the identification (ID) of the first data transmission device (1).

This Page Blank (uspto)

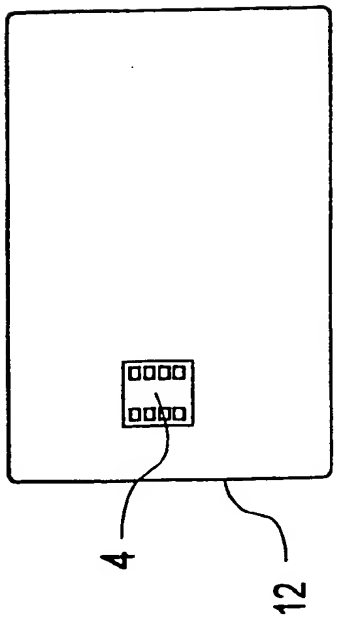

4
12

Fig. 1a

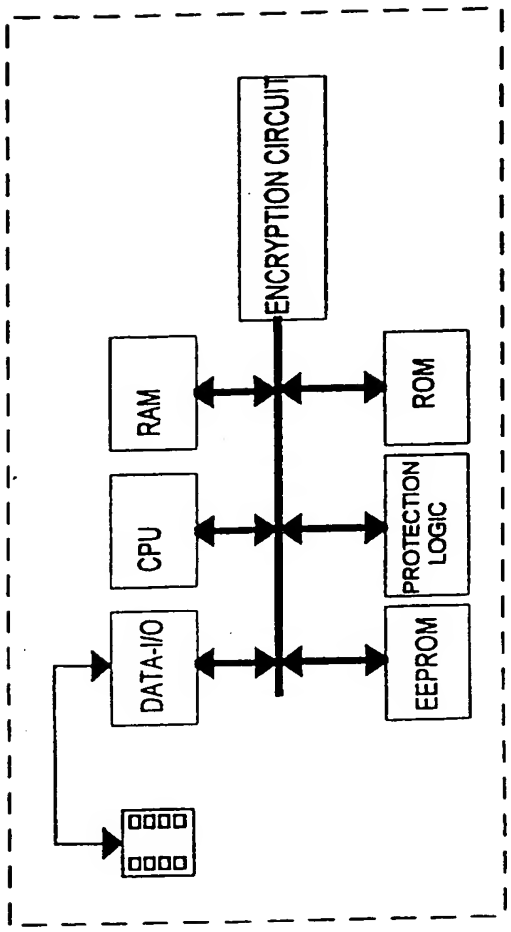

ENCRYPTION CIRCUIT
RAM
ROM
CPU
PROTECTION LOGIC
DATA-I/O
EEPROM

Fig. 1b

This Page Blank (uspto)

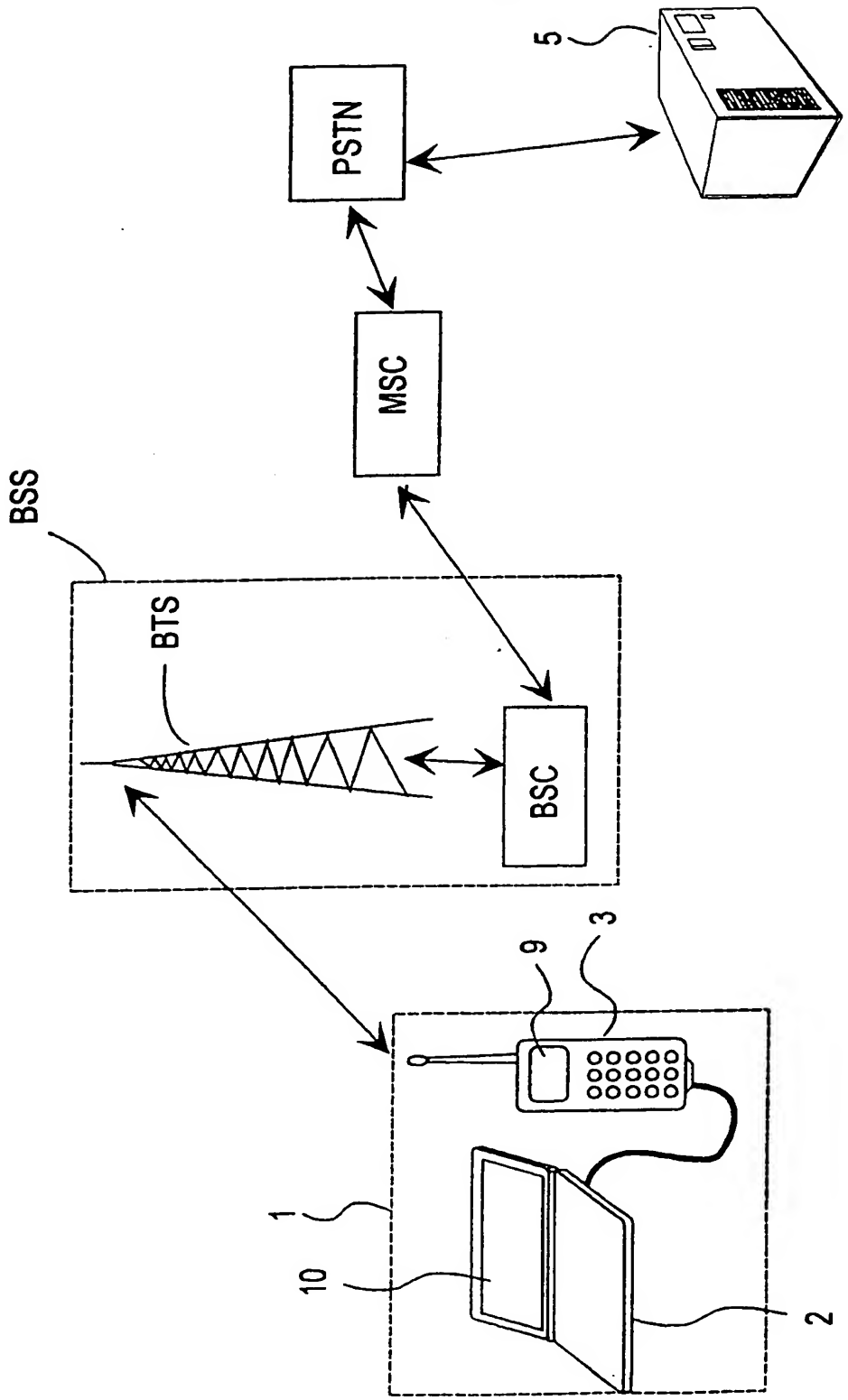


Fig. 2

This Page Blank (uspto)

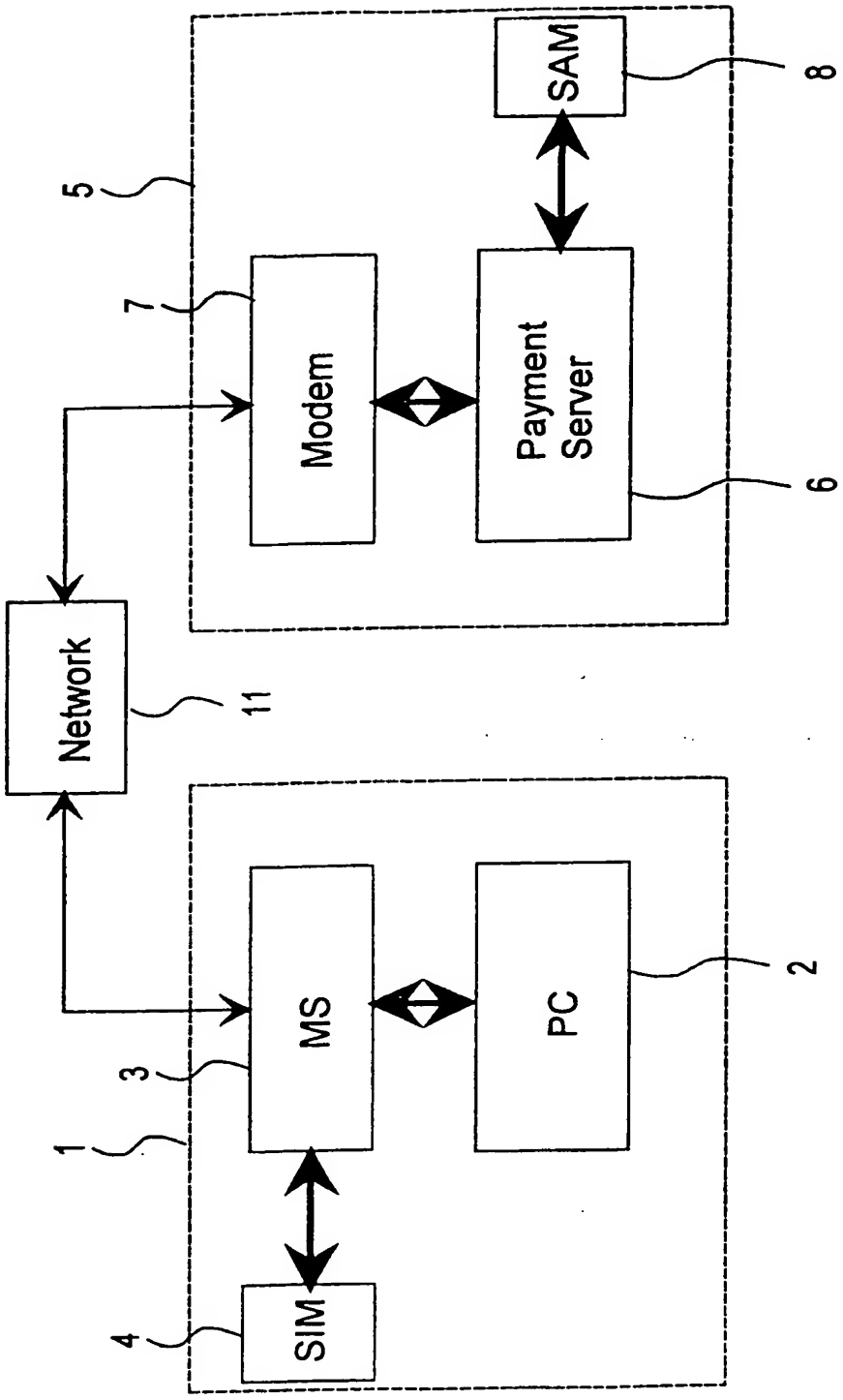


Fig. 3

This Page Blank (uspto)

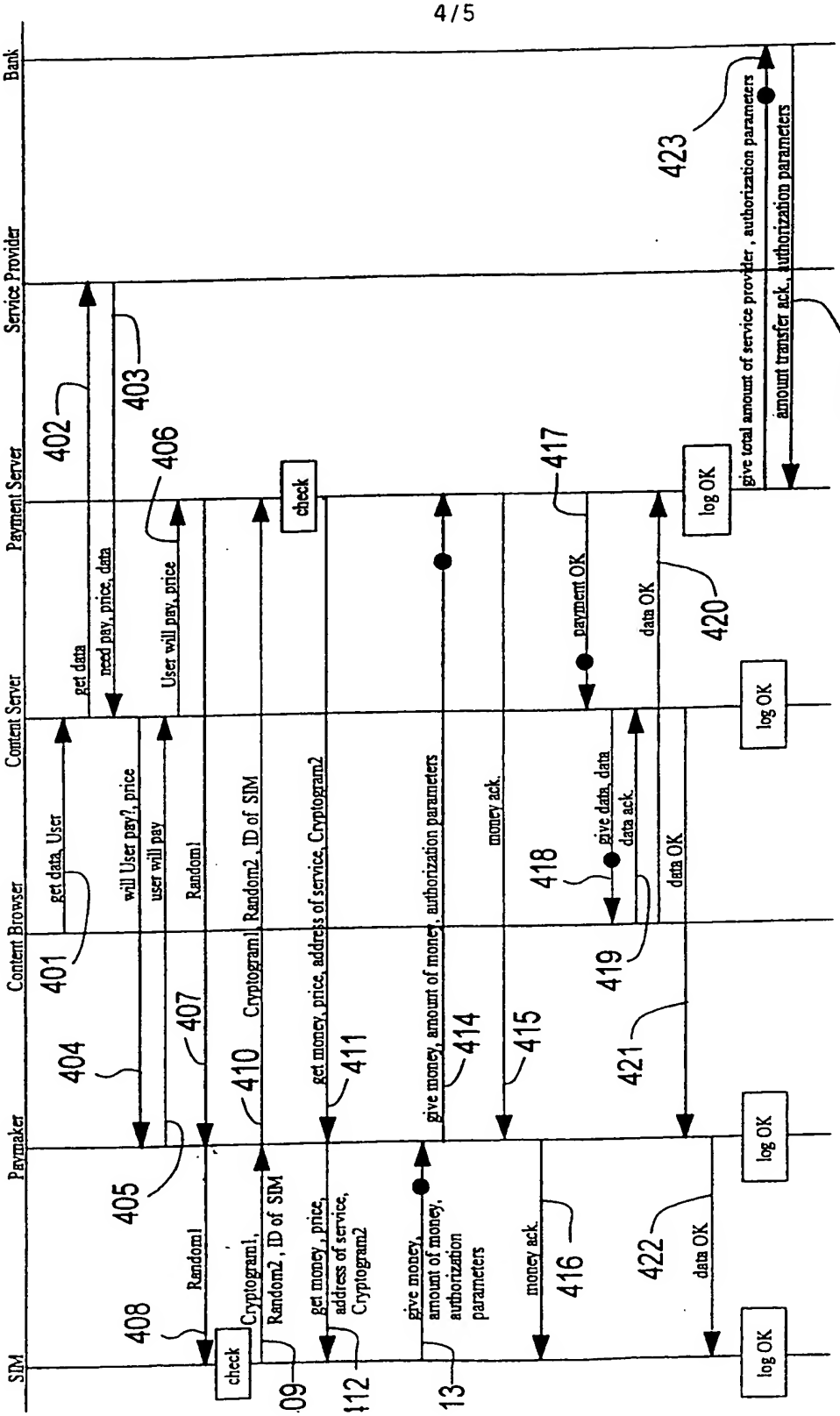

SIM
Paymaker
Content Browser
Content Server
Payment Server
Service Provider
Bank
401
get data, User
will User pay?, price
user will pay
Random1
Random2, ID of SIM
get money, price, address of service, Cryptogram2
give money, amount of money, authorization parameters
money ack.
give data, data
data ack.
data OK
402
get data
need pay, price, data
403
User will pay, price
406
check
407
Cryptogram1, Random2, ID of SIM
410
get money, price, address of service, Cryptogram2
411
give money, amount of money, authorization parameters
414
money ack.
415
payment OK
417
data OK
420
log OK
give total amount of service provider, authorization parameters
423
amount transfer ack., authorization parameters
424
log OK
log OK
log OK
log OK
404
405
Random1
408
check
Cryptogram1, Random2, ID of SIM
09
get money, price, address of service, Cryptogram2
112
give money, amount of money, authorization parameters
13
money ack.
416
418
419
421
422
data OK

Fig. 4

This Page Blank (uspto)

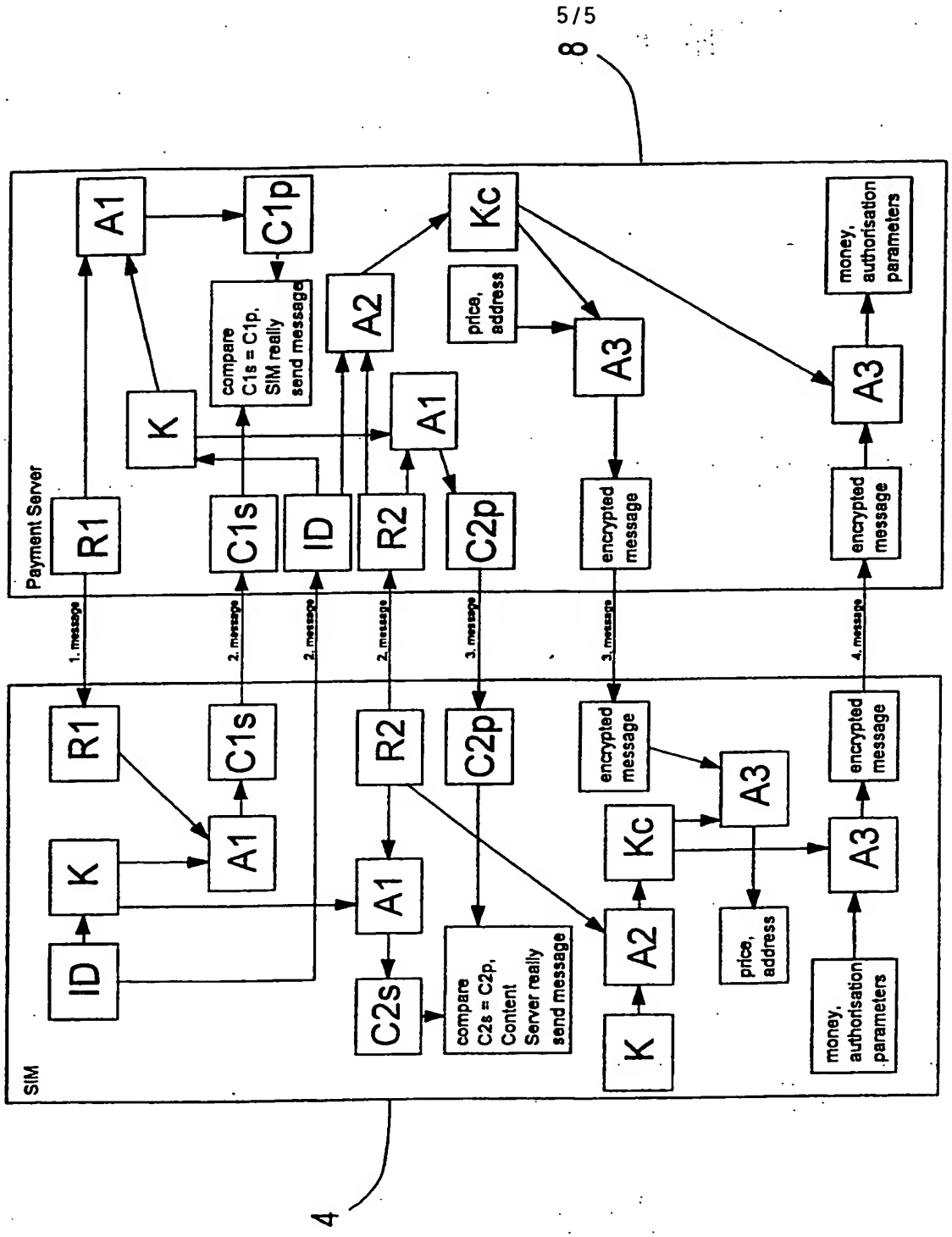

8
Payment Server
A1
C1p
Kc
money, authorisation parameters
compare C1s = C1p, SIM really send message
A2
price, address
A3
K
A1
A3
R1
C1s
ID
R2
C2p
encrypted message
encrypted message
1. message
2. message
2. message
2. message
3. message
3. message
4. message
R1
C1s
R2
C2p
encrypted message
encrypted message
A3
K
A1
Kc
A3
ID
A1
A2
price, address
C2s
compare C2s = C2p, Content Server really send message
K
money, authorisation parameters
SIM
4

Fig. 5

This Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 97/00793

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/32, H04M 1/66
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L, H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5237612 A (ALEX K. RAITH), 17 August 1993 (17.08.93), column 14, line 13 - line 44; column 17, line 6 - line 34	1-8
X	US 5544245 A (HIDEKI TSUBAKIYAMA), 6 August 1996 (06.08.96), column 2, line 50 - column 3, line 21	1-8
X	DE 4442357 A1 (DEUTSCHE TELEKOM AG), 5 June 1996 (05.06.96), column 3, line 37 - line 57	1-8
X	EP 0447380 A1 (TELEFONAKTIEBOLAGET LM ERICSSON), 18 Sept 1991 (18.09.91), column 3, line 6 - column 4, line 17	1-8

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"B" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 June 1998	09 -06- 1998
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Bengt Romedahl Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 97/00793

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5473689 A (GÜNTHER EBERHARD), 5 December 1995 (05.12.95), column 3, line 3 - line 23 -- --------	1-8

INTERNATIONAL SEARCH REPORT

Information on patent family members

29/04/98

International application No.
PCT/FI 97/00793

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5237612 A	17/08/93	EP 0506637 A	30/09/92
US 5544245 A	06/08/96	GB 2279540 A,B	04/01/95
		GB 9411680 D	00/00/00
		JP 6350598 A	22/12/94
DE 4442357 A1	05/06/96	NONE	
EP 0447380 A1	18/09/91	AT 121254 T	15/04/95
		AU 638820 B	08/07/93
		AU 7495291 A	10/10/91
		CA 2051385 A	10/09/91
		CN 1024241 B	13/04/94
		CN 1054868 A	25/09/91
		DE 69008167 D,T	22/09/94
		DE 69108762 D,T	24/08/95
		EP 0460181 A,B	11/12/91
		ES 2073726 T	16/08/95
		FI 915237 B	00/00/00
		HK 101895 A	30/06/95
		IE 67887 B	01/05/96
		JP 4505693 T	01/10/92
		NO 300249 B	28/04/97
		PT 96979 A	30/04/93
		SE 465800 B,C	28/10/91
		SE 9000856 A	10/09/91
		US 5282250 A	25/01/94
		US 5390245 A	14/02/95
		US 5559886 A	24/09/96
		WO 9114348 A	19/09/91
US 5473689 A	05/12/95	AT 162033 T	15/01/98
		DE 4317380 C	18/08/94
		DE 59404924 D	00/00/00
		EP 0631408 A,B	28/12/94

This Page Blank (uspto)

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)